



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/596,924      | 06/19/2000  | THOMAS A. BERSON     | XER1P012            | 4488             |

7590 12/31/2003

Patent Documentation Center  
Xerox Corporation  
100 Clinton Ave. S.  
Xerox Sq. 20th Floor  
Rochester, NY 14644

| EXAMINER |
|----------|
|----------|

MOORTHY, ARAVIND K

| ART UNIT | PAPER NUMBER |
|----------|--------------|
|----------|--------------|

2131

DATE MAILED: 12/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application

09/596,924

Applicant(s)

BERSON ET AL.

Examiner

Aravind K Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 24 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. §§ 119 and 120**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.  
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_ 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**1. Claims 1, 4, 5, 8, 11, 12, 15, 18 and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by Nakamura U.S. Patent No. 5,159,633.**

As to claims 1, 8 and 15, Nakamura discloses receiving a request for a cryptographic service [column 7, lines 1-4]. Nakamura discloses identifying a computational burden required to perform the cryptographic service, including one or more of a privacy level of the cryptographic service or a speed of performing, the cryptographic service. Nakamura discloses determining a price of the cryptographic service based on at least one of computational burden, privacy level, and speed [column 9, lines 55-63].

As to claims 4, 11 and 18, Nakamura discloses requesting payment for the cryptographic service from a user requesting the cryptographic service [column 5, lines 40-52].

As to claims 5, 12 and 19, Nakamura discloses that the cryptographic service includes utilizing private information retrieval [column 5, lines 40-52].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**2. Claims 2, 3, 9, 10, 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura U.S. Patent No. 5,159,633 as applied to claims 1, 8 and 15 above, and further in view of Iwamura U.S. Patent No. 6,272,535 B1.**

As to claims 2, 3, 9, 10, 16 and 17, Nakamura does not teach that a user requesting the cryptographic service specifies the privacy level. Nakamura does not teach a user requesting the cryptographic service specifies the speed of performing the cryptographic service.

Iwamura teaches that a user requesting the cryptographic service specifies the privacy level and speed of performing the cryptographic service [column 15, lines 58-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nakamura so that the user requesting a cryptographic service would have been able to specify the privacy level of the encryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nakamura by the teaching of Iwamura because the examiner asserts that different data needs a different level of privacy based on the sensitivity. So if the price of encryption were dependent on the privacy level then a user with a low priority data would want to pay less for a low level of privacy.

**3. Claims 6, 13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura U.S. Patent No. 5,159,633 as applied to claims 1, 8 and 15 above, and further in view of Billstrom U.S. Patent No. 5,729,537.**

As to claims 6, 13 and 20, Nakamura does not teach that the cryptographic service includes utilizing group authentication.

Billstrom teaches that the cryptographic service includes utilizing group authentication [column 11, lines 22-43].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nakamura so that the cryptographic services included using group authentication.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nakamura by the teaching of Billstrom because group authentication provides anonymous access to the cryptographic service [column 5, lines 5-8].

**4. Claims 7, 14 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura U.S. Patent No. 5,159,633 as applied to claims 1, 8 and 15 above, and further in view of Jakobsson U.S. Patent No. 6,049,613.**

As to claims 7, 14 and 21, Nakamura does not teach that the cryptographic service includes utilizing mix networks.

Jakobsson teaches providing cryptographic services using mix networks [column 5, lines 7-29].

Art Unit: 2131

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nakamura so that the cryptographic services were performed on a mix network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nakamura by the teaching of Jakobsson because mix networks provide superior privacy, robustness, and efficiency [column 2, lines 58-60].

**5. Claims 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura U.S. Patent No. 5,159,633 in view of Ostrovsky et al U.S. Patent No. 5,123,045.**

As to claim 22, Nakamura discloses receiving a request for encrypting a message [column 7, lines 1-4]. Nakamura discloses encrypting the message [column 7, lines 18-26].

Nakamura does not teach that the message is compressed during the encryption. Nakamura does not teach that calculating a price of the encryption is based on the amount of compression.

Ostrovsky et al teaches that the message is compressed during encryption. Ostrovsky et al teaches that calculating a price of the encryption is based on the amount of compression [column 11, lines 23-49].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nakamura so that the messages are compressed during encryption and that the price was calculated based on the amount of compression.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nakamura by the teaching of Ostrovsky et al because the

Art Unit: 2131

examiner asserts that lengthy compression can be expensive, therefore it would be profitable for an encryption service to charge based on the amount of compression.

As to claim 23, Nakamura teaches that the cryptographic service is a digital signature [column 4, lines 9-55].

As to claim 24, Nakamura teaches that the encryption utilizes random bits [column 4, lines 9-55].

### *Conclusion*

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K Moorthy  
December 17, 2003